Cyber-attack modeling analysis techniques: an Overview

Hamad AL-Mohannadi, Qublai Mirza, Anitta Namanya, Irfan Awan, Andrea Cullen and Jules Disso

Abstract - Cyber attack is a sensitive issue in the world of Internet security. Governments and business organisations around the world are providing enormous effort to secure their data. They are using various types of tools and techniques to keep the business running, while adversaries are trying to breach security and send malicious software such as botnets, viruses, trojans etc., to access valuable data. Everyday the situation is getting worse because of new types of malware emerging to attack networks. It is important to understand those attacks both before and after they happen in order to provide better security to our systems. Understanding attack models provide more insight into network vulnerability; which in turn can be used to protect the network from future attacks. In the cyber security world, it is difficult to predict a potential attack without understanding the vulnerability of the network. So, it is important to analyse the network to identify top possible vulnerability list, which will give an intuitive idea to protect the network. Also, handling an ongoing attack poses significant risk on the network and valuable data, where prompt action is necessary. Proper utilisation of attack modelling techniques provide advance planning, which can be implemented rapidly during an ongoing attack event. This paper aims to analyse various types of existing attack modelling techniques to understand the vulnerability of the network; and the behaviour and goals of the adversary. The ultimate goal is to handle cyber attack in efficient manner using attack modelling techniques.

I INTRODUCTION

The Internet in today's society is a key part of human life. We use Internet at home, in the office and on mobile devices anywhere and everywhere we go. It has become important to be connected to Internet 24/7, to keep an eye on business, keep in touch with family and friends, and to keep up to date on news around the world. Being connected does not only concern with the advancement in life or business, it comes with a number of potential danger such as got stolen valuable data, lost privacy or identity, device infected by malware and many more. Everyday the situation is getting worse in the cyber world. Security for any legitimate network is under threat of attack. There are a great number of researchers are working on cyber threat analysis to predict the model of attack for any given network. Some of the researchers have defined these cyber attacks as cyber war [1] and provide some initial guidelines for future defence of cyber space. The defence mechanism mainly concerns with the understanding of their own network, nature of the attacker, motive of the attacker, method of attack, security weakness of the network to mitigate future attacks. To understand the nature of a cyber attack, it is important to model attack earlier to make network more secure, which can be customised depending on the organisation's needs [2].

To detect or handle cyber attack, it is important to learn about the weaknesses of the network. It is also necessary for the cyber security team to understand the motive of the attacker, what data could be targeted and why the attack happened. Proper planning is necessary to deal cyber attack. The attack modelling and analysis has been emphasised in a recent article of Bank of England, which describes how threats can be modelled to mitigate cyber attack in any organisation [3]. Attack modelling techniques are important to understand, explore and validate security threats in the cyber world [4]. BSIMM [2] usages attack modelling techniques in the BSIMM frame work of cyber security. The goal of BSIMM is to use customised knowledge to handle attack in an organisation.

This paper focuses on the cyber attack detection and action upon detection by analysing the well-known analysis techniques. To achieve this goal, we have considered a relevant case study to support the findings.

II ATTACK MODELLING REVIEW

Modelling a cyber attack, which has not happened yet can save time, money and other resources for an organisation. There are a number of attack modelling techniques are used to analyse cyber attack such as Attack Graph or Tree [5] [6], Attack Vector [7], Attack Surface [8], Diamond model [9], OWASP's threat model [4] and Kill Chain[10], [11]. This section focuses on reviewing the three attack modelling techniques called the Diamond Model, the Kill Chain and the Attack Graph for cyber attack modelling. The Diamond Model is selected because of the simplicity of the model as it comprised with only four main components. The Kill Chain is used as it has been used for many years by the US Department of Defence both in cyber defence and in the battle fields. On the other hand, the Attack Graph or Tree is one of the traditional techniques in the computer science which is based on the basic searching ability of a computer system or algorithm [9]. Modelling cyber attack or predicting threat is an important issue for securing any corporate network. The goal of this review is not to compare those techniques but to understand the mechanism to model cyber security threats in order to provide more security in a system.

A. Diamond Model

The Diamond model is one of the novel models for cyber intrusion analysis described in [9] where an adversary attacks a victim depending on two key motivations rather than using a series of steps like the kill chain or the attack graph. This model consists of four basic elements such as adversary, infrastructure, capability and victim. An adversary is an actor (or set of actors) who attacks a victim after analysing their capability against the victim. Initially the adversary starts with no

knowledge of the capability of the victim. After analysing the capability of a victim, the adversary may finds that he/she has more capability than the victim to attack or not. This model is important when dealing with more advanced attackers such as those whom have already gained some control over the network. The adversary also analyse the infrastructure of his/her technical and logical ability to command and control any of victim's network.

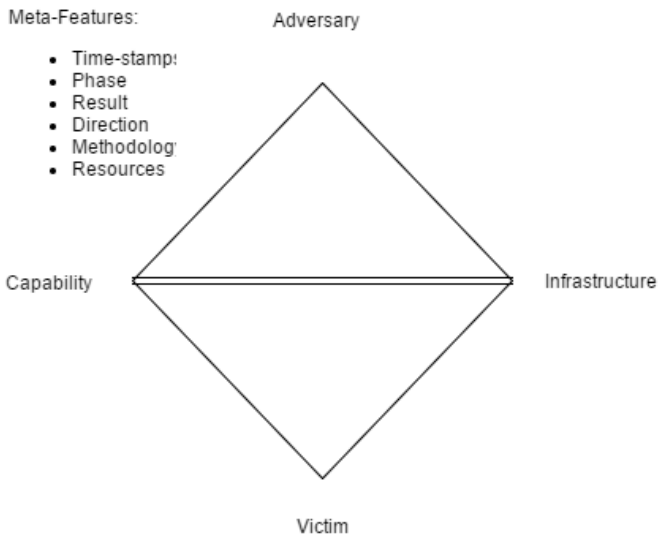

Fig. 1. Diamond Model (Extracted from [9])

The diamond model is also associated with some meta- features such as timestamp, phases, result, directions, methodology and resources. In the event of an attack, the diamond model identifies phases in a timestamp [9]. Components of the diamond model can be found in the figure 1 which illustrates that the adversary looks for opportunity to attack a victim depending on the capability or the infrastructure.

B. Kill Chain

The Kill chain for intrusion is one of the attack modelling techniques, which defines attack as a chain of action. It is a structured attack, since the attacker progresses the attack in an ordered chain according to the plan [11]. The Kill chain technique is described by the US Department of Defence to attack a target [12], where they have defined the Kill Chain with some stages such as, find, fix, track, target, engage and assess. The Kill Chain has been applied in other areas including Cyber Security. In cyber security, [13] it is used to describe some attack steps within a counter measure framework. The research has led the Kill Chain to have seven steps of attack, which can be described below as -

Step 1 Reconnaissance: The attacker gathers information before an attack. The information could be collected from the Internet, which is publicly available.

Step 2 Weaponization: The attacker creates a malicious payload to send to the victim. The payload could be a virus, a trojan or an executable file that can perform some action on the victims' machine or on the network.

Step 3 Delivery: Attacker sends the malicious payload to the victim using some means of communication. The attacker may send the payload via email as an attachment or a link that will download the payload.

Step 4 Exploitation: In this stage the actual exploitation happens. If the victim has download the payload into his/her computer the main exploitation starts. This is the stage where the attacker needs the aid of the victim. Also, this is one of the phases where the chain can be killed by not downloading the payload that the adversary sends.

Step 5 Installation: Install malware on the infected or victims' computer. To infect the victim's computer, the payload may need to be executed by the victim, or it can be automatically executed. This is also the phase where the chain can be broken by not executing the payload.

Step 6 Command and control: Through the installed malware, the attacker creates a command and control channel to access the internal assets of the victim. In this phase the attacker has successfully gained control of the victims' machine.

Step 7 Action on objectives: Attackers achieve their goal on the victims computer or network that is infected. This could be the gateway of the attack. The attacker may progress towards valuable data from the database

through the web server.

The Kill chain is divided into two major phases called left of exploit or hack and right of exploit or hack. In figure 2 we can explore the kill chain steps, where we can see that the left part gives victim an opportunity to kill the chain. If the attacker managed to move on to the right part, it will be difficult for the victim to stop such attack or reduce loss.

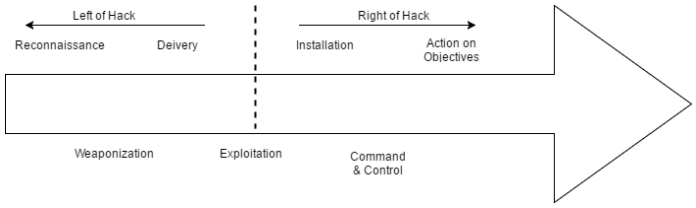

Fig. 2. Kill Chain Attach Modelling (Inspired by [11])

The left part is the initial phase where an adversary will try to gain control of the system. For example, an adversary wants to gain access to a system; he/she will start reconnaissance, i.e., investigating the victims network, profile and other profiles available on the Internet [14]. Let us assume that the adversary has managed to gain the email address of the victim. The email may become the gateway to enter the victims system or network. The adversary will be weaponised in various ways such as social engineering. Common weapons could be trojanised PDF, PPT,DOC, BNP etc., type files sent to the victim as an attachment. The sender tries to be as legitimate as they can. They may also put a link to click. The email subject, id and domain name should look like the real one. Once the email is delivered the adversary waits for the victim's response. In this situation the victim may download the attachment or click the link, or just delete the mail on suspicion. Exploitation plays a vital role in this situation as, if the victim clicks or downloads, the kill chain will advance i.e., malware will be executed on victim's machine.

In this context, it is clear that the left-exploit/hack is the most important for cyber defence for any organization or individual. From the left-hack analysis, we can find a number of insights of such attacks. It can indicate the attackers pattern of attack, sending IP, email domain; location and other relevant information can be collected for defending the victim. Also, understanding the pattern of the attacker, and organization can educate employees on how to deal with such an attack. In most cases, a kill chain can be broken at an early stage in this kind of situation. Understanding the kill chain can help organisations to protect themselves from potential Cyber attacks.

C. Attack Graph

Attack graphs are conceptual diagrams used to analyze how a target can be attacked. This is important to analyze cyber threats on a computer system or network. An attack graph is a tree-structured graph, which has multilevel children with a single root. The Attack Graph or Tree is a traditional way of finding vulnerability, which is introduced by many people including [5] [6] to develop a tool for effective defence by analysing network. The graph essentially consists of nodes and can be complex in nature when dealing with a specific attack. It may contain thousands of nodes with a number of different paths. Generating attack graphs is computationally complex [15] especially in the case of large networks. There are a number of attack graph generating tools and techniques such as TVA (Topological Analysis of Network Attack Vulnerability) [16], NETSPA (A Network Security Planning Architecture) [17] and MULVAL (Multihost, multistage, Vulnerability Analysis) [18] as reviewed in [19]. These tools helps to draw logical attack graphs to understand "why an attack happens?" rather than "how an attack happens?". The main idea of an attack graph is the path from the attackers to the victim's network. Attack graph techniques help to detect intrusions and the vulnerability of the system. An example of attack graph is illustrated in the figure 4 to represent the given case scenario. Attack graphs can be useful in many areas of computer network security including intrusion detection, forensic analysis, risk analysis and cyber defence. A network administrator uses an attack graph to identify

- The vulnerability of the system
- How an attack can happens
- A set of actions that will prevent an attacker in achieving their goal

The main advantage of an attack graph is that it helps to identify any potential attacks on the network. The analysis helps to identify necessary steps if there is any weak point in the network. Using this technique it is possible to calculate Return on Investment (RoI) for security. Organisations mainly avoid security or vulnerability checking because it is expensive [16]. On the other hand, if the cost is too high for the company to afford, it is unlikely that the company will go for an expensive option. So, companies need a clear vision of investment on cyber security.

Generating an attack graph is challenging task, as there are hundreds of nodes that can be involved in the graph, which makes it difficult to identify a valid attack threat. Also there are a number of uncertainties involved in the attack graph

technique. To deal with these uncertainties, some researchers use the Monte Carlo algorithm [15] as it can deal with uncertainty and has statistical dependents. Other algorithms, such as breadth fast and depth fast algorithms are also used to create graph. There are a good number of theoretical works that have been done in the area of attack graph generation. There are some researchers who use Ontology involving entities, properties, relationships and rules to model cyber attack [20].

III CASE STUDY

In this section, we use a case study to analyse these three well-known attack modelling techniques. The goal of this analysis is to identify how each of the models behave when encountering a cyber attack.

The case study involves a victim, who works for a company; and a normal user of a computer. The victim receives an email which has an attachment of a Portable Executable (PE) file with an extension of .exe. The employee has executed the file unknowingly on a company desktop. The email was sent to the company mail with a professional subject line. The attack is reported to the security department when some unusual behaviour is found on that employee's workstation.

The company's security team has identified an intrusion on the employee workstation, which could be a potential security threat to the organisation's network as a whole.

The workstation has been isolated from the network and has invoked action from a cyber incident expert to investigated the case. The investigator uses different types of attack model techniques to model the attack to enable them to prevent or detect future attacks.

A. Case Analysis with Diamond Model

In the diamond model, there are four main components that are: the Adversary; Capability; Infrastructure; and the victim. From the above attack scenario, we have already identified two of the components called the Adversary and the Victim. We analyses each of the main components for this case, by asking some questions. These questions will be answered as we investigate the case using this model.

Victim:

1) *What was the profile of the person being attacked? (Is it a general attack or is it a targeted attack?)*
   It is important to identify the profile of the person attacked. This gives a general idea of the attack whether the person is a general member of public or someone perceived as important. A targeted attack can use an individual who is a general worker to get to more high profile individuals or to the information needed.
2) *Is the detail of the person being attacked publicly available (e.g. via the Internet)?*
   We may like to know, why this person is being attacked? Are any details online and accessible to the general public? Is there any sensitive information online to attract an attacker? The information, mainly the email address of the person, is not in the public domain.
3) *What was attacked? (Email or anything else)*
   It could give an initial idea of why the attack had taken place by identifying what was attacked. The attacker could attack the victim's email, personal data, bank details etc., which could be the initial step of his/her attack. The attack used the corporate email, which is easy to guess or found in the public domain.
4) *Was the person attacked at work, i.e., inside the corpo- rate network?*
   The attack took place in the corporate network as the victim has opened the email in the corporate network. Generally, a corporate network is more secure than a private one. Also, it is assumed that the work email will be accessed at work. So, this gives more opportunity to an attacker to attack a corporate network.

Capability:

1) *Did the attacker use any Malware?*
   A Malware attack could be dangerous for any corporate or personal network. Especially, a Malware attack could ruin the company's reputation or even close the business. The attacker used a malware through a .exe file in a Windows 2007 computer.
2) *If yes, was the malware trying to exploit a vulnerability?* There are thousands of different types of Malware in the cyber world. If we can identify, the type of the malware, it could give an idea about the goal of the attack or the motivation of the attacker [21]. This is a portable executable file, which is commonly used within a Windows PC environment.
3) *How sophisticated is the malware?*
   Since, .exe files are Windows's native executable file, the user usually does not mistrust the file. Generally, it is dangerous as anyone can execute such a file within a computer with little or no user authentication.
4) *Did the malware require human intervention?*
   The malware that requires human intervention; e.g., the user needs to click and allow an install or to execute the malware or the malware may come with an email attachment; and the user needs to click to open it and then the malware executes. Also, the user must have some privileges on the system to execute such files.
5) *Did the attacker use a known hacking tool?*
   Attackers usually use hacking tools to originate an attack. It is important to know if the attacker used any known hacking tool to model or understand the attack. It is unknown if the Adversary has used any hacking tool. In this

case, it is possible that the attacker has used a hacking tool to create the malware. It is possible that the attacker has other hacking tool to use for command and control if the installation is fully successful.

6) *Did the attacker use stolen credentials?*
   It is common to steal credentials before initiating any cyber attack. The attacker used only one email address, which could or could not be stolen.
7) *Is that malware part of a campaign?*

No, this malware was not a part of a campaign, it is just an executable which could potentially make harm to a corporate network to steal data.

Infrastructure:

1) *What IP was used?*
   It is important to identify the IP address of the attacker, which will tell a story about the attack.
   The IP address used in this attack is 191.234.4.50:80 and 176.31.128.232:1443. We can also see a port 80 is used which indicates an email address. On the other hand, port 1443 is one of the main TCP protocols, which is used to transmit the file.
2) *Can the IP be traceable? (Was it a VPN, proxy, etc.)?* The IP needed to be traced to find the source of the attack. The IP that has been used can be traced using a simple trace command in the Windows command prompt.
3) *How many IPs were involved?*
   There were two IP addresses were used in this attack event.
4) *Was a domain name used?*
   Yes, an email must contain a domain name. So, the domain name used in the email was not any legitimate domain.
5) *Can we track that domain name?*
   Yes we can track the domain name.
6) *Can we establish a history for the domain name?*
   Yes, domain history can be identified from the attacker's email address.
7) *Can we find an email related to the attacker?*
   The email address of the attacker was found in the incoming email to the victim. The email address helps to identify the domain name and other relevant details of the attacker.
8) *Are they using a botnet?*
   No, they were not using any botnet, it was an .exe file for the Windows operating systems.
9) *Are we able to find a command and control?*
   The attack was identified and appropriate action have been taken in the early stage. The attacker did not get much time to use any command and control for this attack. Usually, a command and control occurs after the malware been installed in the system. In this case, the action has been taken right after the installation of the executable file.
10) *Is there anything in the malware sample that will tell us about the Infrastructure?* The malware comes with many details; e.g. the malware was an .exe file, which is a Windows based executable file. To create an executable file such as .exe. requires a Windows operating system. So, it is clear that the attacker has used a Windows based infrastructure to perform this attack. Since the attacker has used two IP addresses, it can be assumed that the attacker has well-structured infrastructure.

Adversary:

1) *Can we identify an email from the attacker?*
   To identify an email from an adversary is not an easy task for normal users. The user trusts the email is coming from a legitimate email address.
2) *What physical infrastructure was being used (hardware, operating system, Software version)?*
   It is a very difficult task to identify what kind of infrastructure has been used by the attacker as we cannot physically see any of his activities. Despite this barrier, some components of the infrastructure can be worked out, such as an .exe is generated by Windows Operating Systems, TCP is the common protocol for most Internet communications.
3) *What sort of network was being used (Wi-Fi, private, public servers online)?*
   It could not be identified what sort of network has been used by the attacker during the attack.

Using the Diamond model, we have identified a number of insights into the case study. It is important to ask a number of questions and try to find answers during investigation. This process gives a very clear idea of the attack. In the previous section, we have a number question to investigate the case, which essentially gave deeper insight. In this section, we discuss the findings of the investigation for each of the attack modelling techniques.

In this case study, the Adversary has sent an email to an employee of a company. The email had an attached .exe file and sent to attack the victim's computer or the network. The diamond model allowed us to identify the structure of the attack. For example, the attacker has used the victim's email address and sent an email, which looks like a legitimate one. It could be suggested that the infrastructures are the same for both the victim and the adversary; however, their capabilities differ substantially. The adversary has taken this opportunity to attack an employee of the company not an administrator. A network administrator has knowledge in identifying .exe files from any unknown

source. This indicates that the adversary has done some research on the company or the employee and acquired the knowledge of their infrastructure and capability. So, it is clear that the attacker has used the capability measure of the Diamond attack model to manipulate the victim. In the figure 3 illustrates the abstract view of the attack using diamond model.

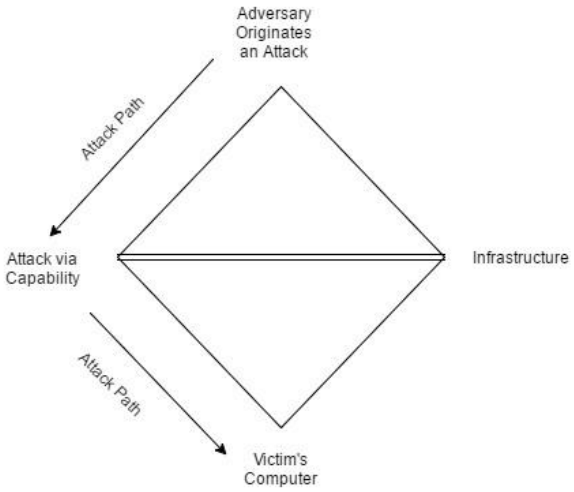

Fig. 3. Attack Path with in the Diamond Model

B. Case Analysis with the Kill Chain

In this section, we analyse an attack using the Kill Chain to understand more about the attack. As previously stated, the Kill Chain has seven steps i.e., the attacker needs to go through those steps to achieve their goals. In this case study, the attacker did not attack the victim directly without doing any research. In the following we have used the earlier case study to analyse the Kill Chain -

Step 1 Reconnaissance: The attacker has gathered lots of information from the Internet and other media in which he/she can reach the goal. It is possible that the attacker's main goal is to access information about the company. One to achieve this is to collect information about an employee of the company. We can say that the attacker has collected an employee email address as an entry point. It is almost impossible to detect the reconnaissance, but worth understanding by the defender before becoming victim. By understanding this phase, it will be easier to protect the network from any attack.

Step 2 Weaponization: The attacker creates a malicious pay- load to send to the victim. The payload is mainly the .exe file, which is a Portable Executable (PE) file. A PE can be executed in Windows operating systems just by clicking. So, this is an easy way to weaponise for the attack. This is the phase that is difficult to recognise by the victim. Although, it is not recognisable, it can be identified by the malware analysis or other investigation. Detecting the weaponiser can play an important role securing a network or understanding a cyber attack.

Step 3 Delivery: An attacker sends the malicious payload to the victim using some means of communication which in this case is an email. So, the attacker has sent PE through email the victim may execute the file.
This is the phase in which the victim has the opportunity to protect themselves from any potential attack. In the case under study, the victim receives the file, which is not under the control of the attacker anymore. It depends entirely on the victim if they want to execute it or not. If the victim does not execute the file(PE), the adversary will not be able to move on to the next step for exploitation.

Step 4 Exploitation: In this stage the actual exploitation happens. The file has been downloaded onto the victim's computer and is ready to be installed. After downloading a file in a computer, the file stays in the computer's memory. In most case, it requires human intervention to execute the file. However, most of the operating systems notify if the user really want to install the particular software.

Step 5 Installation: The file has been installed by the victim, which makes the attacker's job easy. In this step, the victim should be more careful before installing any unwanted software. Modern Windows operating systems always ask before installing any software from an unknown source. So, to prevent any cyber attack, the victim should check the credentials of the software.

Step 6 Command and control: Through the installed malware, the attacker creates a command and control channel to

access the internal asset of the victim. The attacker may get control over the DNS, websites, social networks or other methods. The command may gather information from the infected computer or its network. The method of data collection could be keystroke monitoring, password cracking, screen capture, sneak into valuable documents etc., to capture valuable information.

Step 7 Action on objectives: The attacker achieves their goal on the victims infected computer or network.

From the victim's side it is not possible to see how the attacker attempts an attack. It could only be anticipated from the kill chain method that the attacker has taken those steps. If we go reverse order to the chain from the attack, it could become clear that the attacker took time to research before doing any attack. The attacker also tries different types of methods such as social engineering by sending an email. The attack could be cut off from Step 3, which is Delivery by understanding the malicious activities of an attacker. If the attacker managed to go to Step 7, which is the goal of the attack, they can do whatever they plan. Once the attack is recognised, it is possible to understand all the steps of the attack and find the pattern of such attacks.

C. Case Analysis with Attack Graph

In attack graph technique, the attacker can attack using many different paths to get control of the victim's network. The attacker could be anywhere on the Internet when origi- nating an attack. In our case study, the attacker attacks using social engineering techniques to get access to the victim's computer. The attack graph for the attack scenario can be summarised as below -

- Adversary stays on the Internet and creates a Portable Executable (PE). The adversary has done enough research to collect information about the victim. The file has been created to attack a particular network. The file contains the goal or the motive of the attacker including the attack information.
- The Adversary researches online into the organisation to be attacked. The information gathered is available in the public domain. The adversary usually takes time to get information for making any valid attack.
- The adversary identifies an employee email address as an entry point. An attacker always needs an entry point that will help in achieving their goal.
- An email is sent to the employee with a PE with an assumption that the employee will open and download the file. This a plan of the adversary, which needs victims intervention to be successful.
- If the employee executes the PE, the adversary can exploit the Workstation of the employee. This exploitation could get more information about the network as well as the web server or other connected devices,(e.g. flash drives), attached to the workstation.

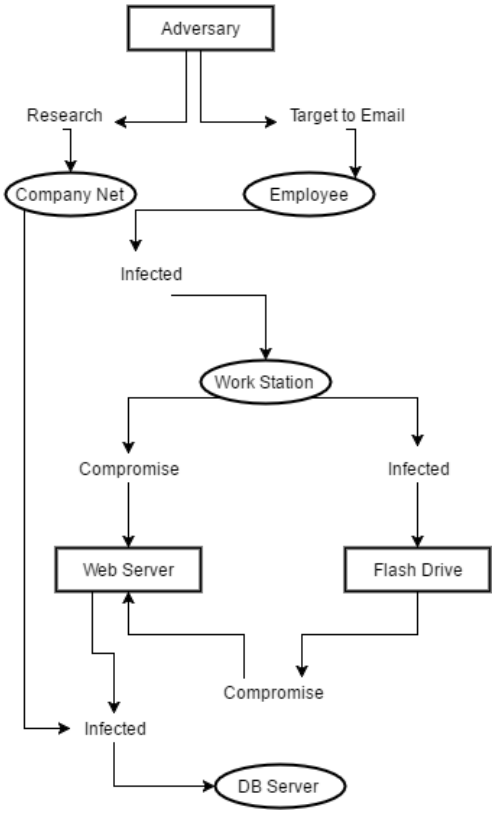

Fig. 4. Attack Graph Technique

- Gradually the attack can be extended to the ultimate goal such as the manipulation of a database server using the web server or a DDoS attack.

In general to model an attack, the attack graph technique requires the deployment of a graph that shows a number of attack paths. These paths could hold information that can be used to prevent future cyber attacks within a high-profile network. In the figure 4 we have modeled the attack for our case study, in which we can see the a number of attack paths to reach victim's database server. There could be a number of paths from the adversary to the victim, it depends on how the secure the victim's infrastructure is. In figure 4, we can see that the adversary can access the database server, if he/she can infect the company core network. This path is very challenging as the company security system may not be compromised and an alert could be generated. So, the cyber security team may increase the security to prevent potential cyber attack. The attacker has selected the other path, which is via an employee. In this path the attacker has to go through many steps, once in the company network, but gives more probability to success on attack goal. Analysing each of the path could lead to the vulnerabilities of any organisation's network. So, in this method, we have identified the victim employee worked as a gateway, which helps the adversary to proceed further with the attack.

IV Discussion

Using these three models to analyse the same cyber attack is useful. Each of the methods is unique and presents the same attack in very different ways. In this section, we discuss the insight achieved following this analysis using three attack modelling techniques.

The diamond model has only four components with a number of subcomponents. The diamond shows that the adversary has more capability than the victim. The victim has executed the PE on the machine to allow the adversary to achieve the goal. On the other hand, the adversary is not as strong as the PE in this aspect, as the file cannot be executed without any user intervention. The attack could be prevented if the victim could identify the executable file as malicious earlier. The victim's computer is a part of the victim's infrastructure, which may be as stronger as the adversary's one, however the knowledge of the victim played as a weak point in this situation. So, in this case, it is clear that the victim may have same strength in the infrastructure as the attacker but weaker in capability.

The kill chain method gives more details of the attack using seven steps. These steps are like a chain, which can be broken from the victim's side as soon as an incident is reported. First three steps cannot be controlled by the victim. From the step 3, the victim can kill the chain if a threat is recognised from it payload. The payload, which could be a malware that can give information about the motive of the attacker. On the other hand, reverse engineering the kill chain could help security team to identify the behaviour and motivation of the attacker. These indications could help the network to be more secure by finding the weak points.

The attack graph is generated to identify the vulnerability of the system, understand how an attacked happened and to set actions to prevent further attacks. The graph gives multiple paths that an attack has happened in any network. This technique can also help to identify potential threats by analysing the network vulnerability. Analysing network vulnerability using attack graph technique is expensive as generating a graph is difficult. There are a number of tools available for creating graph. In our case analysis, we have illustrated graph using the attack scenario. This graph shows the current path of the attack as well as relevant branches that could be infected.

Although, the attack modelling techniques are different from each other, they share some common attributes such as adversary, victim, network, attack plan, create payload, delivery of the payload installation and execution. One of the important parts of any cyber attack is that the attacker does not attack on any high-profile network without doing proper research. The attacker plans before making attack. The plan is done using collected data on victim's infrastructure and capability. To make an attack the attacker needs to send a payload, in our case the .exe file, which is very common way of attacking any Windows workstation. Also, a social engineering method is used to deliver the payload to victim. So, the chance of success is fifty-fifty, because once the file is delivered, it is upon the victim whether to execute or not. The attack graph shows if the attacker makes a successful attack, there will be more alternative ways will be opened for making further attack such as Distributed Denial of Service (DDoS).

V CONCLUSION AND FUTURE WORK

In this paper we have demonstrated three attack modelling techniques to analyse a case of cyber attack. In this simple case analysis, we have identified that cyber attacks can be modelled using different techniques. Each of the techniques gives interesting insights about a cyber attack. For example, the diamond model identifies how and why an attack happens, as we can see that an attacker attacks an victim depending on two main attributes called Infrastructure and Capability. The attacker will attack a victim if the victim's capability or the infrastructure is weaker. An attack event will not be successful if the victim is stronger than the attacker in Infrastructure and Capability. On the other hand, the kill chain technique gives detail steps of an attack. Although, the attacker considers the infrastructure and capability before originating any attack, the victim gets opportunity to kill the attack chain, if attack is identified in any of the early stages. So, it is important that the victim is aware of the attack chain. The attack graph indicates that how many ways cyber attacks can be happened. An attack

graph technique finds multiple path that can lead to a cyber attack to any company network infrastructure. Each of the path can represent some vulnerability information. To mitigate network vulnerability the attack graph technique can help securing a complex corporate network from any potential cyber attack.

In the future work, we aim to extend to model cyber attack more effectively. One of the dimensions of this extension could be setting up honeypots to extract attack data. These attack data could be analysed by using appropriate tool to find attack pattern. These attack patterns could be used to implement with these mentioned attacked modelling techniques for better understanding of cyber attack. Advanced Persistent Threat (APT) is one of the issue in the cyber security world [22]. In this case, a group of attackers use full planning advanced infrastructure and capability to attack a corporate network. This is a growing and challenging issue for the businesses and governments. Another dimension of this research could be analysing APT using honeypots data and attack modelling techniques.

REFERENCES

[1] M. Golling and B. Stelte, "Requirements for a future ews-cyber defence in the internet of the future," in *Cyber conflict (ICCC), 2011 3rd international conference on*. IEEE, 2011, pp. 1–16.

[2] BSIMM, "Attack models with bsimm frameworks," *Online*, vol. https://www.bsimm.com/framework/intelligence/attack-models/, 2016.

[3] B. of England, "Cbest intelligence-led testing- an introduction to cyber threat modelling," *Bank of England Publication*, vol. http://www.bankofengland.co.uk/anintroductiontocbest.pdf, 2016.

[4] X. Lin, P. Zavarsky, R. Ruhl, and D. Lindskog, "Threat modeling for csrf attacks," *2013 IEEE 16th International Conference on Computational Science and Engineering*, vol. 3, pp. 486–491, 2009.

[5] C. Phillips and L. P. Swiler, "A graph-based system for network-vulnerability analysis," in *Proceedings of the 1998 Workshop on New Security Paradigms*, ser. NSPW '98. New York, NY, USA: ACM, 1998, pp. 71–79. [Online]. Available: http://doi.acm.org/10.1145/310889.310919

[6] B. Schneier, "Attack trees," *Dr. Dobbs journal*, vol. 24, no. 12, pp. 21– 29, 1999.

[7] M. Mulazzani, S. Schrittwieser, M. Leithner, M. Huber, and E. R. Weippl, "Dark clouds on the horizon: Using cloud storage as attack vector and online slack space." in *USENIX Security Symposium*. San Francisco, CA, USA, 2011, pp. 65–76.

[8] P. K. Manadhata and J. M. Wing, "An attack surface metric," *Software Engineering, IEEE Transactions on*, vol. 37, no. 3, pp. 371–386, 2011.

[9] S. Caltagirone, A. Pendergast, and C. Betz, "The diamond model of intrusion analysis," DTIC Document, Tech. Rep., 2013.

[10] U. S. J. C. of Staff, *Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace*. Joint Chiefs of Staff, 2000.

[11] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," *Leading Issues in Information Warfare & Security Research*, vol. 1, p. 80, 2011.

[12] W. L. Sharp, "Joint publication 3-60: Joint targeting," *Washington DC: Joint Chiefs of Staff*, 2007.

[13] T. Sakuraba, S. Domyo, B.-H. Chou, and K. Saku, "Exploring security countermeasures along the attack sequence," in *Information Security and Assurance, 2008. ISA 2008. International Conference on*. IEEE, 2008, pp. 427–432.

[14] N. Ghosh and S. K. Ghosh, "A planner-based approach to generate and analyze minimal attack graph," *Applied Intelligence*, vol. 36, no. 2, pp. 369–390, 2012.

[15] V. Shandilya, C. B. Simmons, and S. Shiva, "Use of attack graphs in security systems," *Journal of Computer Networks and Communications*, vol. 2014, 2014.

[16] N. STEVEN and S. JAJODIA, "Measuring security risk of networks us- ing attack graphs," *International Journal of NextGeneration Computing*, vol. 1, no. 1, 2010.

[17] R. Lippmann, "Netspa: A network security planning architecture," *Massachusetts Institute of Technology*, 2002.

[18] X. Ou, S. Govindavajhala, and A. W. Appel, "Mulval: A logic-based network security analyzer." in *USENIX security*, 2005.

[19] X. Ou and A. Singhal, "Attack graph techniques," in *Quantitative Security Risk Assessment of Enterprise Networks*. Springer, 2011, pp. 5–8.

[20] L. Obrst, P. Chase, and R. Markeloff, "Developing an ontology of the cyber security domain." in *STIDS*, 2012, pp. 49–56.

[21] M. Sikorski and A. Honig, *Practical malware analysis: the hands-on guide to dissecting malicious software*. no starch press, 2012.

[22] P. Chen, L. Desmet, and C. Huygens, "A study on advanced persistent threats," in *Communications and Multimedia Security*. Springer, 2014, pp. 63-72.